



FIGURE 1

T13C1D9814|BYE5|DIC0A802FF|DP8|IDU0|EP800|PK1|PR11|S|C0A80263|SP8A
T13C1D9821|BY5C|DIC0A80215|IDU3C|EP806|PK2|SA0000E8DA99DC|S|C0A80201
T13C1D9834|BY4E|DIC0A802FF|DP89|IDU0|EP800|PK1|PR11|S|C0A80297|SP89
T13C1D9839|BY114|IDU3A|EP1|F|PK6
T13C1D9878|BYA6|IDU0|EP A6|PK1
T13C1D9878|BYE5|DIC0A802FF|DP8|IDU0|EP800|PK1|PR11|S|C0A80297|SP8A
T13C1D987E|BY114|IDU3A|EP1|F|PK6
T13C1D988E|BY148|DIC0A80219|DP43|IDU0|EP800|PK1|PR11|S|C0A80299|SP44
T13C1D988E|BY148|DIC0A80299|DP44|IDU0|EP800|PK1|PR11|S|C0A80219|SP43
T13C1D988E|BY2E|DIC0A80219|IDU0|EP806|PK1|SA009027078E8E|S|C0A80299

FIGURE 2

---Timestamp

TI-start-time in seconds (since 1970 GMT)

DU-duration of validity (for time grouping)

---Structural Fields

GB-indicator that this row is an output of grouping operation

MP-indicator that this row is a mapping or lookup row

---Key Fields (this category includes Secondary Key Fields):

CD-collection device (i.e. origin of the data)

DA-destination MAC address (as stated by ARP packet)

DD-destination domain (DNS style)

DI-destination IP number

DM-destination MAC address (true MAC address)

DN-normalised destination address

DP-destination TCP port or UDP port

EP-Ethernet protocol number

PR-IP protocol number

SA-source MAC address (as stated by ARP packet)

SD-source domain (DNS style)

SI-source IP number

SM-source MAC address (true MAC address)

SN-normalised source address

SP-source TCP port or UDP port

---Secondary Key Fields (actually, special case of Key Fields)

TF-traffic flow

AC-account category

SA-sub-account category

CC-cost centre category

---Counter fields

BY-count of bytes

PK-count of packets

HT-count of web hits

FIGURE 3